COUNTING NONSINGULAR MATRICES WITH PRIMITIVE ROW VECTORS

SAMUEL HOLMIN

Abstract. We give an asymptotic expression for the number of nonsingular integer $n\times n$-matrices with primitive row vectors, determinant k, and Euclidean matrix norm less than T, as $T \to \infty$.

We also investigate the density of matrices with primitive rows in the space of matrices with determinant k, and determine its asymptotics for large k.

1. Introduction

An integer vector $v \in \mathbb{Z}^n$ is **primitive** if it cannot be written as an integer multiple $m \neq 1$ of some other integer vector $w \in \mathbb{Z}^n$. Let A be an integer $n \times n$-matrix with nonzero determinant k and primitive row vectors. We ask how many such matrices A there are of Euclidean norm at most T, that is, $\|A\| \leq T$, where $\|A\| := \sqrt{\sum a_{ij}^2} = \sqrt{\operatorname{tr}(A^t A)}$. Let $N'_{n,k}(T)$ be this number (the prime in the notation denotes the primitivity of the rows), and let $N_{n,k}(T)$ be the corresponding counting function for matrices with not necessarily primitive row vectors. We will determine the asymptotic behavior of $N'_{n,k}(T)$ for large T, and investigate the density $D_n(k) := \lim_{T\to\infty} N'_{n,k}(T)/N_{n,k}(T)$ of matrices with primitive vectors in the space of matrices with determinant $k \neq 0$.

Let $M_{n,k}$ be the set of integer $n\times n$-matrices with determinant k. Then $N_{n,k}(T) = |B_T \cap M_{n,k}|$, where B_T is the (closed) ball of radius T centered at the origin in the space $M_n(\mathbb{R})$ of real $n\times n$-matrices equipped with the Euclidean norm. Throughout, we will assume that $n \geq 2$ and $k > 0$ unless stated otherwise.

Duke, Rudnick and Sarnak [DRS93] found that the asymptotic behavior of $N_{n,k}$ is given by

$$N_{n,k}(T) = c_{n,k} T^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(n+1)+\varepsilon}),$$

as $T \to \infty$, for a certain constant $c_{n,k}$ and all $\varepsilon > 0$, where the error term can be improved to $O(T^{4/3})$ for $n = 2$. The corresponding case for singular matrices was later investigated by Katznelson, who proved in [Kat93] that

$$N_{n,0}(T) = c_{n,0} T^{n(n-1)} \log T + O(T^{n(n-1)}).$$

See the next page for the constants $c_{n,k}$ and $c_{n,0}$.

Let $M'_{n,k}$ be the set of matrices in $M_{n,k}$ with primitive row vectors. Then $N'_{n,k}(T) = |B_T \cap M'_{n,k}|$. Wigman [Wig05] determined the asymptotic behavior of the counting function $|G_T \cap M'_{n,0}|$, where G_T is a ball of radius T in $M_n(\mathbb{R})$, under a slightly different norm than ours. The results can be transferred to our setting,

Date: November 13, 2012.

The author was partially supported by the Swedish Research Council.

whereby we have

$$\begin{aligned}
N'_{n,0}(T) &= c'_{n,0}T^{n(n-1)}\log T + O(T^{n(n-1)}), \qquad n \geq 4,\\
N'_{3,0}(T) &= c'_{3,0}T^{3(3-1)}\log T + O(T^{3(3-1)}\log\log T),\\
N'_{2,0}(T) &= c'_{2,0}T^{2(2-1)} + O(T).
\end{aligned}$$

The case $n = 2$ above is equivalent to the **primitive circle problem**, which asks how many primitive vectors there are of length at most T in $\mathbb{Z}^2$ given any (large) T.

The main result in our paper is the following asymptotic expression for the number of nonsingular matrices with primitive row vectors and fixed determinant.

Theorem 1. *Let $k \neq 0$. Then*

$$N'_{n,k}(T) = c'_{n,k}T^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon}),$$

as $T \to \infty$ for a certain constant $c'_{n,k}$ and all $\varepsilon > 0$.

Section 3 is dedicated to the proof of this theorem.

The constant in Theorem 1 can be written as

$$c'_{n,k} = \frac{C_1}{|k|^{n-1}} \sum_{d_1\cdots d_n=|k|} \prod_{i=1}^{n} \sum_{g|d_i} \mu(g)\left(\frac{d_i}{g}\right)^{i-1},$$

for $k \neq 0$, which may be compared to the constants obtained from [DRS93], [Kat93] and [Wig05], namely

$$\begin{aligned}
c_{n,k} &= \frac{C_1}{|k|^{n-1}} \sum_{d_1\cdots d_n=|k|} \prod_{i=1}^{n} d_i^{i-1}\\
c_{n,0} &= C_0\frac{n-1}{\zeta(n)}\\
c'_{n,0} &= \begin{cases} C_0\dfrac{n-1}{\zeta(n-1)^n\zeta(n)} & (n \geq 3)\\ \dfrac{\pi T^2}{\zeta(2)} & (n = 2)\end{cases}
\end{aligned}$$

where ζ is the Riemann zeta function, μ is the Möbius function, and C_0 and C_1 are constants defined as follows (these depend on n, but we will always regard n as fixed). Let ν be the normalized Haar measure on $\mathrm{SL}_n(\mathbb{R})$. The measure w below is obtained by averaging the $n(n-1)$-dimensional volume of $E \cap A_u$ over all classes $A_u := \{A \in M_n(\mathbb{R}) : Au = 0\}$ for nonzero $u \in \mathbb{R}^n$. In Appendix A we give a precise definition of w and calculate $w(B_1)$.

Write V_n for the volume of the unit ball in $\mathbb{R}^n$ and S_{n-1} for the surface area of the $(n-1)$-dimensional unit sphere in $\mathbb{R}^n$. Then

$$\begin{aligned}
C_0 &:= w(B_1) = \frac{V_{n(n-1)}S_{n-1}}{2} = \frac{\pi^{n^2/2}}{\Gamma\left(\frac{n}{2}\right)\Gamma\left(\frac{n(n-1)}{2}+1\right)},\\
C_1 &:= \lim_{T\to\infty}\frac{\nu(B_T \cap \mathrm{SL}_n(\mathbb{R}))}{T^{n(n-1)}} = \frac{V_{n(n-1)}S_{n-1}}{2\zeta(2)\cdots\zeta(n)} = \frac{C_0}{\zeta(2)\cdots\zeta(n)}.
\end{aligned}$$

1.1. **Density.** It will be interesting to compare the growth of $N'_{n,k}$ to that of $N_{n,k}$. We define the **density** of matrices with primitive rows in the space $M_{n,k}$ to be

$$D_n(k) := \lim_{T\to\infty}\frac{N'_{n,k}(T)}{N_{n,k}(T)} = \frac{c'_{n,k}}{c_{n,k}}.$$

The asymptotics of $N_{n,0}$ and $N'_{n,0}$ are known from [Kat93] and [Wig05], and taking their ratio, we see that

$$D_n(0) = \frac{1}{\zeta(n-1)^n}$$

for $n \geq 3$. We will be interested in the value of $D_n(k)$ for large n and large k. The limit of $D_n(k)$ as $k \to \infty$ does not exist, but it does exist for particular sequences of k.

We say that a sequence of integers is **totally divisible** if its terms are eventually divisible by all positive integers smaller than m, for any m. We say that a sequence of integers is **rough** if its terms eventually have no divisors smaller than m (except for 1), for any m. An equivalent formulation is that a sequence $(k_1, k_2, \ldots)$ is totally divisible if and only if $|k_i|_p \to 0$ as $i \to \infty$ for all primes p, and $(k_1, k_2, \ldots)$ is rough if and only if $|k_i|_p \to 1$ as $i \to \infty$ for all primes p, where $|m|_p$ denotes the p-adic norm of m.

We state our main results about the density D_n. We prove these in section 4.

Theorem 2. *Let $n \geq 3$ be fixed. Then D_n is a multiplicative function, and $D_n(p^m)$ is strictly decreasing as a function of m for any prime p. We have*

$$D_n(0) < D_n(k) < D_n(1)$$

for all $k \neq 0, 1$. Now let $k_1, k_2, \ldots$ be a sequence of integers. Then

$$D_n(k_i) \to 1$$

if and only if $(k_1, k_2, \ldots)$ is a rough sequence, and

$$D_n(k_i) \to \frac{1}{\zeta(n-1)^n}$$

if and only if $(k_1, k_2, \ldots)$ is a totally divisible sequence. Moreover, $D_n(k) \to 1$ uniformly as $n \to \infty$.

We prove Theorem 2 for nonzero k_i, but it is interesting that this formulation holds for $k = 0$ also. The case of $k = 0$ was proved by Wigman [Wig05], where he found that $D_n(0)$ equals $1/\zeta(n-1)^n$. We remark that Theorem 2 implies that

$$D_n(k_i) \to D_n(0)$$

if and only $(k_1, k_2, \ldots)$ is totally divisible, for any fixed $n \geq 3$.

For completeness, let us state what happens in the rather different case $n = 2$.

Proposition 3. *Let $n = 2$. Then D_n is a multiplicative function, and $D_n(p^m)$ is strictly decreasing as a function of m for any prime p. We have*

$$D_2(k_i) \to 0$$

if and only if $\lim_{i \to \infty} \sum_{p|k_i} 1/p \to \infty$. Moreover,

$$D_2(k_i) \to 1$$

if and only if $\lim_{i \to \infty} \sum_{p|k_i} 1/p \to 0$. The sums are taken over all primes p which divide k_i.

1.2. **Proof outline.** Our proof of Theorem 1 uses essentially the same approach as [DRS93]. The set $M'_{n,k}$ is partitioned into a finite number of orbits $A\,\mathrm{SL}_n(\mathbb{Z})$, where $A \in M_{n,k}$ are matrices in Hermite normal form with primitive row vectors. We count the matrices in each orbit separately. The number of matrices in each orbit scales as a fraction $1/k^{n-1}$ of the number of matrices in $\mathrm{SL}_n(\mathbb{Z})$. We can view $\mathrm{SL}_n(\mathbb{Z})$ as a lattice in the space $\mathrm{SL}_n(\mathbb{R})$, and the problem is reduced to a lattice point counting problem. The lattice points inside the ball B_T are counted by evaluating the normalized Haar measure of $B_T \cap \mathrm{SL}_n(\mathbb{R})$.

1.3. **Acknowledgements.** I would like to thank my advisor Pär Kurlberg for suggesting this problem to me and for all his help and encouragement.

2. Preliminaries

The **Riemann zeta function** ζ is given by

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - 1/p^s}$$

for $\operatorname{Re} s > 1$, where we use the convention that when an index p is used in a sum or product, it ranges over the set of primes.

The **Möbius function** μ is defined by $\mu(k) := (-1)^m$ if k is a product of m distinct prime factors (that is, k is **square-free**), and $\mu(k) := 0$ otherwise. We note that μ is a **multiplicative function**, that is, a function $f : \mathbb{N}^* \to \mathbb{C}$ defined on the positive integers such that $f(ab) = f(a)f(b)$ for all coprime a, b.

We will use the fact that $\mathrm{SL}_n(\mathbb{R}) = M_{n,1}$ has a normalized Haar measure ν which is bi-invariant (see [Sie45]).

2.1. **Lattice point counting.** Let G be a topological group with a normalized Haar measure ν_G and a lattice subgroup $\Gamma \subseteq G$, and let G_T be an increasing family of bounded subsets of G for all $T \geq 1$. Under certain conditions (see for instance [GN10]), we have

$$|G_T \cap \Gamma| \sim \nu_G(G_T \cap G),$$

where we by $f(T) \sim g(T)$ mean that $f(T)/g(T) \to 1$ as $T \to \infty$. In this paper, we are interested in the lattice $\mathrm{SL}_n(\mathbb{Z})$ inside $\mathrm{SL}_n(\mathbb{R})$, and the following result will be crucial.

Theorem 4 ([DRS93], Theorem 1.10)**.** *Let B_T be the ball of radius T in the space $M_n(\mathbb{R})$ of real $n \times n$-matrices under the Euclidean norm $\|A\| = \sqrt{\operatorname{tr}(A^t A)}$. Let ν be the normalized Haar measure of $\mathrm{SL}_n(\mathbb{R})$. Then*

$$|B_T \cap \mathrm{SL}_n(\mathbb{Z})| = \nu(B_T \cap \mathrm{SL}_n(\mathbb{R})) + O_\varepsilon(T^{n(n-1)-1/(n+1)+\varepsilon})$$

for all $\varepsilon > 0$, and the main term is given by

$$|B_T \cap \mathrm{SL}_n(\mathbb{Z})| \sim C_1 T^{n(n-1)}, \quad C_1 = \frac{1}{\zeta(2)\cdots\zeta(n)} \frac{\pi^{n^2/2}}{\Gamma\left(\frac{n}{2}\right)\Gamma\left(\frac{n(n-1)}{2}+1\right)}.$$

In fact, a slightly more general statement is true. We can replace the balls B_T in Theorem 4 with balls under any norm on $M_n(\mathbb{R})$, and the asymptotics will still hold, save for a slighty worse exponent in the error term.

Theorem 5 ([GN10], Corollary 2.3)**.** *Let $\|\cdot\|'$ be any norm on the vector space $M_n(\mathbb{R})$, and let G_T be the ball of radius T in $M_n(\mathbb{R})$ under this norm. Let ν be the normalized Haar measure of $\mathrm{SL}_n(\mathbb{R})$. Then*

$$|G_T \cap \mathrm{SL}_n(\mathbb{Z})| = \nu(G_T \cap \mathrm{SL}_n(\mathbb{R})) + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon})$$

for all $\varepsilon > 0$.

We will be interested in the following particular case of Theorem 5. Let $A \in M_{n,k}$. Then $\|X\|' := \|A^{-1}X\|$ defines a norm on $M_n(\mathbb{R})$, and the ball of radius T in $M_n(\mathbb{R})$ under the norm $\|\cdot\|'$ is $A \cdot B_T$.

Corollary 6. *Let $A \in M_{n,k}$. Then*

$$|AB_T \cap \mathrm{SL}_n(\mathbb{Z})| = \nu(AB_T \cap \mathrm{SL}_n(\mathbb{R})) + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon})$$

for all $\varepsilon > 0$, using the notation from Theorem 4.

3. The number of matrices with primitive rows

In the present section, we will prove Theorem 1. We begin by noting that the divisors of each row in an integer $n \times n$-matrix A are preserved under multiplication on the right by any matrix $X \in \mathrm{SL}_n(\mathbb{Z})$. In particular, if each row of A is primitive, then each row of AX is primitive, for any $X \in \mathrm{SL}_n(\mathbb{Z})$. So we get:

Lemma 7. *If $A \in M'_{n,k}$ then $AX \in M'_{n,k}$ for all $X \in \mathrm{SL}_n(\mathbb{Z})$. Thus $A \cdot \mathrm{SL}_n(\mathbb{Z}) \subseteq M'_{n,k}$.*

Consequently $M'_{n,k}$ may be written as a disjoint union of orbits of $\mathrm{SL}_n(\mathbb{Z})$:

$$M'_{n,k} = \bigcup_{A \in \mathcal{A}} A\,\mathrm{SL}_n(\mathbb{Z}),$$

for properly chosen subsets $\mathcal{A}$ of $M'_{n,k}$. In fact, as we will show in the following, the number of orbits is finite, and so we may take $\mathcal{A}$ to be finite.

A lower triangular integer matrix

$$C := \begin{pmatrix} c_{11} & 0 & \cdots & 0 \\ c_{21} & c_{22} & \ddots & 0 \\ \vdots & & \ddots & 0 \\ c_{n1} & \cdots & c_{n(n-1)} & c_{nn} \end{pmatrix}$$

is said to be in (lower) **Hermite normal form** if $0 < c_{11}$ and $0 \le c_{ij} < c_{ii}$ for all $j < i$. The following result is well-known.

Lemma 8 ([Coh93], Theorem 2.4.3)**.** *Assume $k > 0$. Given an arbitrary matrix $A \in M_{n,k}$, the orbit $A\,\mathrm{SL}_n(\mathbb{Z})$ contains a unique matrix C in Hermite normal form.*

We may thus write

$$M'_{n,k} = \bigcup_{i=1}^{m} A_i\,\mathrm{SL}_n(\mathbb{Z}),$$

where $A_1, \dots, A_m$ are the unique matrices in Hermite normal form with primitive row vectors and determinant k, and $m := |M'_{n,k}/\,\mathrm{SL}_n(\mathbb{Z})|$. By counting the number of matrices in Hermite normal form with determinant $k > 0$, we get

$$|M_{n,k}/\,\mathrm{SL}_n(\mathbb{Z})| = \sum_{d_1 \cdots d_n = k} d_1^0 d_2^1 \cdots d_n^{n-1}, \tag{9}$$

where the sum ranges over all positive integer tuples $(d_1, \dots, d_n)$ such that $d_1 \cdots d_n = k$.

Proposition 10. *Let $k > 0$. Then*

$$|M'_{n,k}/\,\mathrm{SL}_n(\mathbb{Z})| = \sum_{d_1 \cdots d_n = k} \prod_{i=1}^{n} \sum_{g | d_i} \mu(g) \left(\frac{d_i}{g}\right)^{i-1}$$

where the first sum ranges over all positive integer tuples $(d_1, \dots, d_n)$ such that $d_1 \cdots d_n = k$.

Proof. We want to count those matrices in Hermite normal form which are in $M'_{n,k}$, that is, $n \times n$-matrices in Hermite normal form with determinant k and all rows primitive. The number of such matrices is

$$\left|M'_{n,k}/\,\mathrm{SL}_n(\mathbb{Z})\right| = \sum_{d_1 \cdots d_n = k} \prod_{i=1}^{n} v_i(d_i),$$

where $v_i(d)$ is the number of primitive vectors $(x_1, \dots, x_{i-1}, d)$ such that $0 \le x_1, \dots, x_{i-1} < d$. There is a bijective correspondence between the primitive vectors

$(x_1, \dots, x_{i-1}, d)$ and the vectors $y = (y_1, \dots, y_{i-1})$ such that $1 \le y_1, \dots, y_{i-1} \le d$ and $\gcd(y)$ is coprime to d. Let $d = p_1^{a_1} \cdots p_j^{a_j}$ be the prime factorization of d. The number of vectors y which are divisible by some set of primes $P \subseteq \{p_1, \dots, p_j\}$ is

$$\left(\frac{d}{\prod_{p \in P} p} \right)^{i-1},$$

so by the principle of inclusion/exclusion (see [Sta97]), we have

$$\begin{aligned} v_i(d) &= \sum_{P \subseteq \{p_1, \dots, p_j\}} (-1)^{|P|} \left(\frac{d}{\prod_{p \in P} p} \right)^{i-1} \\ &= \sum_{g \mid p_1 \cdots p_j} \mu(g) \left(\frac{d}{g} \right)^{i-1} = \sum_{g \mid d} \mu(g) \left(\frac{d}{g} \right)^{i-1}. \end{aligned}$$

□

We are now ready to derive the asymptotics of $N'_{n,k}(T)$.

Proof of Theorem 1. Let us write $A_1, \dots, A_m$ for all the $n \times n$-matrices in Hermite normal form with determinant k, where $m := |M'_{n,k} / \operatorname{SL}_n(\mathbb{Z})|$, and let $1 \le i \le m$. Then

$$|B_T \cap A_i \operatorname{SL}_n(\mathbb{Z})| = \left| A_i (A_i^{-1} B_T \cap \operatorname{SL}_n(\mathbb{Z})) \right| = \left| A_i^{-1} B_T \cap \operatorname{SL}_n(\mathbb{Z}) \right|,$$

which by Corollary 6 is equal to

$$\nu(A_i^{-1} B_T \cap \operatorname{SL}_n(\mathbb{Z})) + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon})$$

for any $\varepsilon > 0$. Since $A_i / k^{1/n} \in \operatorname{SL}_n(\mathbb{R})$, we get by the invariance of the measure ν that

$$\begin{gathered} \nu(A_i^{-1} B_T \cap \operatorname{SL}_n(\mathbb{Z})) = \nu \left(\frac{A_i}{k^{1/n}} \left(A_i^{-1} B_T \cap \operatorname{SL}_n(\mathbb{R}) \right) \right) = \\ \nu \left(k^{-1/n} B_T \cap \frac{A_i}{k^{1/n}} \operatorname{SL}_n(\mathbb{R}) \right) = \nu \left(B_{T/k^{1/n}} \cap \operatorname{SL}_n(\mathbb{R}) \right). \end{gathered}$$

By Theorem 4, the last expression is equal to

$$C_1 (T/k^{1/n})^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon}),$$

and thus

$$|B_T \cap A_i \operatorname{SL}_n(\mathbb{Z})| = \frac{C_1}{k^{n-1}} T^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon}). \tag{11}$$

Now,

$$N'_{n,k}(T) = \left| B_T \cap M'_{n,k} \right| = \left| B_T \cap \bigcup_{i=1}^m A_i \operatorname{SL}_n(\mathbb{Z}) \right| = \sum_{i=1}^m |B_T \cap A_i \operatorname{SL}_n(\mathbb{Z})|,$$

so applying (11) we get

$$\begin{gathered} N'_{n,k}(T) = \sum_{i=1}^m \frac{C_1}{k^{n-1}} T^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon}) = \\ \left| M'_{n,k} / \operatorname{SL}_n(\mathbb{Z}) \right| \frac{C_1}{k^{n-1}} T^{n(n-1)} + O_\varepsilon(T^{n(n-1)-1/(2n)+\varepsilon}), \end{gathered}$$

and we need only apply Proposition 10 to get an explicit constant for the main term. This concludes the proof. □

4. Density of matrices with primitive rows

Set

$$a_n(k) := |M_{n,k}/\operatorname{SL}_n(\mathbb{Z})| = \sum_{d_1\cdots d_n=k} d_1^0\cdots d_n^{n-1}, \tag{12}$$

$$a_n'(k) := |M_{n,k}'/\operatorname{SL}_n(\mathbb{Z})| = \sum_{d_1\cdots d_n=k}\prod_{i=1}^n\sum_{g\mid d_i}\mu(g)\left(\frac{d_i}{g}\right)^{i-1}. \tag{13}$$

We would like to calculate the density of matrices with primitive rows in $M_{n,k}$ for $k\neq 0$, that is, the quantity

$$D_n(k) = \lim_{T\to\infty}\frac{N_{n,k}'(T)}{N_{n,k}(T)} = \frac{c_{n,k}'}{c_{n,k}} = \frac{|M_{n,k}'/\operatorname{SL}_n(\mathbb{Z})|}{|M_{n,k}/\operatorname{SL}_n(\mathbb{Z})|} = \frac{a_n'(k)}{a_n(k)}.$$

We will prove in section 4.1 that a_n, a_n' and D_n are multiplicative functions, and therefore we need only understand their behavior for prime powers $k=p^m$. We will now prove a sequence of lemmas which we will finally use in section 4.2 to prove Theorem 2.

Lemma 14. *The functions a_n' and a_n are connected via the identity*

$$a_n'(p^m) = \sum_{i=0}^m(-1)^i\binom{n}{i}a_n(p^{m-i})$$

for primes p and $m\geq 0$.

Proof. $a_n(p^m)$ counts the number of $n\times n$-matrices in Hermite normal form with determinant p^m, whereas $a_n'(p^m)$ counts the number of such with primitive rows. If A is a matrix that $a_n(p^m)$ counts which $a_n'(p^m)$ does not, then some set of rows, indexed by $S\subseteq[n]:=\{1,\dots,n\}$ (where $|S|\leq m$), are divisible by p. The number of such matrices is $a_n(p^{m-|S|})$, and thus by the inclusion/exclusion principle,

$$a_n'(p^m) = \sum_{\substack{S\subseteq[n]\\|S|\leq m}}(-1)^{|S|}a_n(p^{m-|S|}) = \sum_{i=0}^m(-1)^i\binom{n}{i}a_n(p^{m-i}). \qquad \square$$

Lemma 15. *For any prime p and $m\geq 1$, the following recursion holds:*

$$a_n(p^m) = p^{n-1}a_n(p^{m-1}) + a_{n-1}(p^m),$$

or equivalently,

$$a_n(p^{m-1}) = \frac{a_n(p^m)-a_{n-1}(p^m)}{p^{n-1}}.$$

Proof. We split the sum

$$a_n(p^m) = \sum_{d_1\cdots d_n=p^m} d_1^0\cdots d_n^{n-1}$$

into two parts, one part where d_n is divisible by p, and another part where it is not (so that $d_n=1$). The terms corresponding to $d_n=1$ sum to $a_{n-1}(p^m)$. Where d_n is divisible by p, we can write $d_n =: pe_n$ for some e_n. Let $e_i := d_i$ for all $i<n$. Thus,

$$\sum_{\substack{d_1\cdots d_n=p^m\\p\mid d_n}} d_1^0\cdots d_n^{n-1} = \sum_{e_1\cdots e_n=p^{m-1}} e_1^0\cdots(e_n/p)^{n-1} = \frac{1}{p^{n-1}}a_n(p^{m-1}).$$

Adding the two parts gives us $a_n(p^m)=p^{n-1}a_n(p^{m-1})+a_{n-1}(p^m)$, from which the claim in the lemma follows by rearrangement. $\square$

Lemma 16. *Let n and p be fixed, where $n \geq 3$ and p is a prime. Then*
$$D_n(p^m) \to \left(1 - \frac{1}{p^{n-1}}\right)^n$$
as $m \to \infty$.

Proof. We apply the simple upper bound
$$a_{n-1}(p^m) = \sum_{d_1 \cdots d_{n-1} = p^m} d_1^0 \cdots d_n^{n-2} \leq \sum_{d_1 \cdots d_{n-1} = p^m} (p^m)^{n-2} = (m+1)^{n-1}(p^m)^{n-2}$$
to the expression for $a_n(p^{m-1})$ in Lemma 15:
$$\begin{aligned} a_n(p^{m-1}) &= \frac{1}{p^{n-1}}(a_n(p^m) - a_{n-1}(p^m)) \\ &= \frac{1}{p^{n-1}} a_n(p^m) + O((p^m)^{n-2}(m+1)^{n-1}). \end{aligned}$$
Repeated application (at most n times) of this formula yields the asymptotics
$$a_n(p^{m-i}) = \frac{1}{(p^{n-1})^i} a_n(p^m) + O((p^m)^{n-2}(m+1)^{n-1})$$
for $1 \leq i \leq n$.

Now let $m \to \infty$, so that we may assume m to be larger than n. The sum in Lemma 14 then extends up to $i = n$ (because the factors $\binom{n}{i}$ vanish for larger i), so
$$\begin{aligned} a_n'(p^m) &= \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_n(p^{m-i}) \\ &= \sum_{i=0}^{n} (-1)^i \binom{n}{i} \frac{1}{(p^{n-1})^i} a_n(p^m) + O((p^m)^{n-2}(m+1)^{n-1}). \end{aligned}$$
We divide by $a_n(p^m)$ on both sides and use the fact that $a_n(p^m) \geq (p^m)^{n-1}$, so that
$$\begin{aligned} D_n(p^m) &= \sum_{i=0}^{n} (-1)^i \binom{n}{i} \frac{1}{(p^{n-1})^i} + O\left(\frac{(p^m)^{n-2}(m+1)^{n-1}}{(p^m)^{n-1}}\right) \\ &= \sum_{i=0}^{n} \binom{n}{i} \left(\frac{-1}{p^{n-1}}\right)^i + O\left(\frac{(m+1)^{n-1}}{p^m}\right) \\ &= \left(1 - \frac{1}{p^{n-1}}\right)^n + O\left(\frac{(m+1)^{n-1}}{p^m}\right). \end{aligned}$$
As $m \to \infty$, the second term on the right vanishes. □

4.1. **Proof that $D_n(p^m)$ is strictly decreasing.** In this section we will prove the following proposition.

Proposition 17. *The function D_n is multiplicative, and $D_n(p^m)$ is strictly decreasing as a function of m for any fixed prime p and dimension $n \geq 2$.*

We may rewrite (12) as
$$a_n = (\cdot)^{n-1} * \cdots * (\cdot)^0$$
where $(\cdot)^i$ is the function $x \mapsto x^i$ and $*$ denotes the Dirichlet convolution. Similarly, we may rewrite (13) as
$$a_n' = (\mu * (\cdot)^{n-1}) * \cdots * (\mu * (\cdot)^0),$$
so by the commutativity and associativity of the Dirichlet convolution we have
$$a_n' = \mu^{*n} * a_n,$$

where μ^{*n} denotes the convolution of μ with itself n times (so that $\mu^{*1} = \mu$). Since the Dirichlet inverse of μ is the constant function 1, we have also the relation

$$a_n = 1^{*n} * a'_n.$$

As μ and $(\cdot)^i$ are multiplicative functions, it follows that a_n, a'_n and D_n are multiplicative as well.

Now, we want to show that

$$D_n(p^m) = \frac{a'_n(p^m)}{a_n(p^m)}$$

is strictly decreasing as a function of m, for fixed $n \geq 2$ and primes p, or equivalently that

$$\frac{a'_n(p^m)}{a_n(p^m)} > \frac{a'_n(p^{m+1})}{a_n(p^{m+1})} \tag{18}$$

for all $m \geq 0$.

4.1.1. *The case $m < n$.* The inequality (18) is equivalent to

$$\frac{a'_n(p^m)}{(1^{*n} * a'_n)(p^m)} > \frac{a'_n(p^{m+1})}{(1^{*n} * a'_n)(p^{m+1})}$$

for all $m \geq 0$, which is equivalent to

$$\frac{a'_n(p^m)}{\sum_{i=0}^{m} 1^{*n}(p^i) a'_n(p^{m-i})} > \frac{a'_n(p^{m+1})}{\sum_{i=0}^{m+1} 1^{*n}(p^i) a'_n(p^{m+1-i})},$$

or, after taking the reciprocal of both sides,

$$\sum_{i=0}^{m} 1^{*n}(p^i) \frac{a'_n(p^{m-i})}{a'_n(p^m)} < \sum_{i=0}^{m+1} 1^{*n}(p^i) \frac{a'_n(p^{m+1-i})}{a'_n(p^{m+1})}. \tag{19}$$

Now, a matrix $A \in M'_{n,p^m}$ in Hermite normal form with primitive rows can be mapped uniquely to a matrix $A' \in M'_{n,p^{m+1}}$ by multiplying the largest diagonal element by p, where we break ties by always choosing the diagonal element on the later row. This shows that $m \mapsto a'_n(p^m)$ is a non-decreasing function, and thus all factors $\frac{a'_n(p^{m-i})}{a'_n(p^m)}$ and $\frac{a'_n(p^{m+1-i})}{a'_n(p^{m+1})}$ lie in the interval $(0, 1]$, and since also 1^{*n} is a positive function, the last inequality (19) holds if

$$\sum_{i=0}^{m} 1^{*n}(p^i) \leq 1^{*n}(p^{m+1}).$$

Now, $1^{*n}(p^i)$ is the number of ways of writing i as a sum of n non-negative integers, and it is well-known (see [Sta97]) that this is equal to $\binom{n-1+i}{n-1}$ for all i, so the last inequality is equivalent to

$$\sum_{i=0}^{m} \binom{n-1+i}{n-1} \leq \binom{n+m}{n-1}.$$

A well-known combinatorial identity (see exercise 2.1 in [Sta97]) states that the left side above is equal to $\binom{n+m}{n}$. By the unimodality and symmetry of binomial coefficients, we have $\binom{n+m}{n} \leq \binom{n+m}{n-1}$ if and only if $(n+m)/2 \leq n - 1/2$, which is equivalent to the inequality $m \leq n-1$. We have therefore proven (18) and thus Proposition 17 for $m \leq n-1$.

It remains to prove (18) for $m \geq n$. We begin by making the following observation. The inequality (18) is equivalent to (19), and the inequality (19) holds for $m \geq n$ if

$$\frac{a'_n(p^{m-i})}{a'_n(p^m)} \leq \frac{a'_n(p^{m+1-i})}{a'_n(p^{m+1})},$$

for all $i \leq m$. We can rearrange this inequality as

$$\frac{a'_n(p^{m+1})}{a'_n(p^m)} \leq \frac{a'_n(p^{m+1-i})}{a'_n(p^{m-i})},$$

which states that

$$\frac{a'_n(p^{m+1})}{a'_n(p^m)}$$

is a non-increasing function of $m \geq n$, for fixed $n \geq 2$ and p prime. We will therefore be done if we can prove that

$$a'_n(p^m)a'_n(p^{m+2}) \leq a'_n(p^{m+1})a'_n(p^{m+1}) \tag{20}$$

for all $m \geq n$.

4.1.2. *The case $m \geq n$.* We will now prove (20). Accordingly we will assume $m \geq n$.

We begin by noting that $a_n(p^m)$ can be written as the Gaussian binomial coefficient (see [Sta97])

$$a_n(p^m) = \binom{m+n-1}{n-1}_p = \frac{(p^{m+1}-1)\cdots(p^{m+n-1}-1)}{(p-1)\cdots(p^{n-1}-1)} \tag{21}$$

which may be proved by simply observing that $\binom{m+n-1}{n-1}_p = p^{n-1}\binom{(m-1)+n-1}{n-1}_p + \binom{m+(n-1)-1}{(n-1)-1}_p$ satisfies the recursion formula for $a_n(p^m)$ given in Lemma 15, with the same initial values, and thus must coincide with $a_n(p^m)$.

Now, the numerator $a_n(p^m)\cdot(p-1)\cdots(p^{n-1}-1)$ of (21) equals

$$(p^{m+1}-1)\cdots(p^{m+n-1}-1) = \sum_{i=0}^{n-1}(-1)^{n-1-i}p^{mi}Q_i(p) \tag{22}$$

where for each i we have defined the polynomial

$$Q_i(p) := \sum_{1\leq c_1<\cdots<c_i\leq n-1} p^{c_1+\cdots+c_i},$$

which depends on n but not on m. Thus, using the formula for $a'_n(p^m)$ from Lemma 14, we get

$$\begin{gathered}
a'_n(p^m)\cdot(p-1)\cdots(p^{n-1}-1) = \\
\sum_{j=0}^{n}(-1)^j\binom{n}{j}\sum_{i=0}^{n-1}(-1)^{n-1-i}p^{(m-j)i}Q_i(p) = \\
\sum_{i=0}^{n-1}(-1)^{n-1-i}Q_i(p)p^{mi}\sum_{j=0}^{n}(-1)^j\binom{n}{j}p^{-ji} = \\
\sum_{i=0}^{n-1}(-1)^{n-1-i}Q_i(p)(1-p^{-i})^n p^{mi},
\end{gathered}$$

where we used the fact that for $m \geq n$, the sum over j extends up to $j = n$. Inserting the expression above into (20), we find it remains to prove that

$$\sum_{i=0}^{n-1}(-1)^{n-1-i}Q_i(p)(1-p^{-i})^n p^{mi}\sum_{j=0}^{n-1}(-1)^{n-1-j}Q_j(p)(1-p^{-j})^n p^{(m+2)j} \leq$$
$$\sum_{i=0}^{n-1}(-1)^{n-1-i}Q_i(p)(1-p^{-i})^n p^{(m+1)i}\sum_{j=0}^{n-1}(-1)^{n-1-j}Q_j(p)(1-p^{-j})^n p^{(m+1)j}.$$

This can be rewritten as

$$\sum_{i,j=0}^{n-1}(-1)^{i+j}Q_i(p)Q_j(p)(1-p^{-i})^n(1-p^{-j})^n p^{mi+(m+2)j} \leq$$
$$\sum_{i,j=0}^{n-1}(-1)^{i+j}Q_i(p)Q_j(p)(1-p^{-i})^n(1-p^{-j})^n p^{(m+1)(i+j)}$$

or equivalently

$$0 \leq \sum_{i,j=0}^{n-1}(-1)^{i+j}Q_i(p)Q_j(p)(1-p^{-i})^n(1-p^{-j})^n(p^{(m+1)(i+j)} - p^{mi+(m+2)j}).$$

Since $p^{(m+1)(i+j)} - p^{mi+(m+2)j} = p^{m(i+j)}p^{i+j} - p^{m(i+j)}p^{2j}$, the last inequality is equivalent to

$$0 \leq \sum_{i,j=0}^{n-1}(-1)^{i+j}Q_i(p)Q_j(p)(1-p^{-i})^n(1-p^{-j})^n p^{m(i+j)}(p^{i+j} - p^{2j}).$$

We observe that the diagonal terms $i = j$ vanish, as well as the terms with $i = 0$ and the terms with $j = 0$. Pairing terms (i, j) and (j, i) opposite the diagonal, and observing that $2p^{i+j} - p^{2i} - p^{2j} = -(p^i - p^j)^2$, we get the equivalent inequality

$$0 \leq \sum_{1\leq i<j\leq n-1}(-1)^{1+i+j}Q_i(p)Q_j(p)(1-p^{-i})^n(1-p^{-j})^n p^{m(i+j)}(p^i - p^j)^2. \tag{23}$$

for all $m \geq n$ och all primes p. The sum is empty for $n = 2$, so we may assume that $n \geq 3$. We note that each term in the sum (23) is positive if $i + j$ is odd, and negative if $i + j$ is even, and thus each negative term satisfies $i + 1 < j$. We will show that the sum is non-negative by showing that each negative term with position (i, j) is no larger in absolute value than the positive term with position $(i + 1, j)$. That is,

$$Q_i(p)Q_j(p)(1-p^{-i})^n(1-p^{-j})^n p^{m(i+j)}(p^i - p^j)^2 \leq$$
$$Q_{i+1}(p)Q_j(p)(1-p^{-i-1})^n(1-p^{-j})^n p^{m(i+1+j)}(p^{i+1} - p^j)^2,$$

which is equivalent to

$$Q_i(p)(1-p^{-i})^n(p^i - p^j)^2 \leq$$
$$Q_{i+1}(p)(1-p^{-i-1})^n p^m(p^{i+1} - p^j)^2.$$

We prove the last inequality by comparing the left and right-hand sides factor by factor. We have $i+1 < j \leq n-1$, and thus $i+1 \leq n-1$, and therefore

$$Q_i(p) = \sum_{1 \leq c_1 < \cdots < c_i \leq n-1} p^{c_1 + \cdots + c_i} \leq$$
$$\sum_{1 \leq c_1 < \cdots < c_{i+1} \leq n-1} p^{c_1 + \cdots + c_{i+1}} \left(\frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots \right) \leq$$
$$\sum_{1 \leq c_1 < \cdots < c_{i+1} \leq n-1} p^{c_1 + \cdots + c_{i+1}} = Q_{i+1}(p)$$

since both sums are nonempty and $1/p + 1/p^2 + \cdots \leq 1$ for all $p \geq 2$. We also have

$$(1 - p^{-i})^n \leq (1 - p^{-i-1})^n.$$

Finally, the factor $(p^j - p^i)^2$ is smaller than the factor $p^m(p^j - p^{i+1})^2$, which is demonstrated by the following string of implications

$$p(p-1)^2 > 1 \implies p^3(1-1/p)^2 > 1 \implies$$
$$p^m(1-1/p)^2 > 1 \implies p^m(1 - p^{i+1}/p^j)^2 > 1 \iff$$
$$p^m(p^j - p^{i+1})^2 > (p^j)^2 \implies p^m(p^j - p^{i+1})^2 > (p^j - p^i)^2,$$

which hold for all $m \geq n \geq 3$, $j > i+1$ and $p \geq 2$. Thus (20) is true for all $m \geq n$. This concludes the proof of Proposition (17). $\square$

4.2. **Asymptotics of the density function.** In this section we prove Theorem 2 and thus derive the asymptotics of $D_n(k)$. Fix $n \geq 3$. For any nonzero integer k_i, write $k_i = \prod_p p^{m_p(i)}$ as a product of prime powers, where all but finitely many of the exponents $m_p(i)$ are zero. Then since D_n is multiplicative, we have

$$D_n(k_i) = \prod_p D_n(p^{m_p(i)}).$$

Now, by Lemma 16 and Proposition 17, we get

$$1 \geq \prod_p D_n(p^{m_p(i)}) > \prod_p \left(1 - \frac{1}{p^{n-1}}\right)^n = \frac{1}{\zeta(n-1)^n} > 0,$$

so it follows that $\prod_p D_n(p^{m_p(i)})$ is uniformly convergent with respect to i, and therefore

$$\lim_{i \to \infty} \prod_p D_n(p^{m_p(i)}) = \prod_p \lim_{i \to \infty} D_n(p^{m_p(i)}). \tag{24}$$

Let $(k_1, k_2, \ldots)$ be a sequence of nonzero integers. It now follows from (24), Proposition 17 and the fact that $D_n(1) = 1$, that

$$D_n(k_i) \to 1$$

if and only if $m_p(i) \to 0$ as $i \to \infty$ for all p, that is, if and only if $(k_1, k_2, \ldots)$ is a rough sequence. Likewise it follows, using Lemma (16), that

$$D_n(k_i) \to \frac{1}{\zeta(n-1)^n}$$

if and only if $m_p(i) \to \infty$ for all p, that is, if and only if $(k_1, k_2, \ldots)$ is a totally divisible sequence. Since $D_n(0) = 1/\zeta(n-1)^n$, we may allow the elements of the sequence $(k_1, k_2, \ldots)$ to also assume the value 0.

Finally, it follows that $D_n(k) \to 1$ as $n \to \infty$ uniformly with respect to k since

$$D_n(k) \geq \frac{1}{\zeta(n-1)^n} \to 1$$

as $n \to \infty$ because $\zeta(n-1) = 1 + O(2^{-n})$ for $n \geq 3$. We have thus proved all parts of Theorem 2. $\square$

We conclude this section by proving Proposition 3, which tells us the asymptotics of $D_2(k)$ for $n = 2$.

Proof of Proposition 3. If $m = 0$, we have $D_2(p^m) = 1$. Assume $m > 0$. The 2×2-matrices in Hermite normal form with determinant p^m and primitive rows are of the form $\begin{pmatrix} 1 & 0 \\ x & p^m \end{pmatrix}$ where $0 \leq x < p^m, p \nmid x$. Thus $a_2'(p^m) = p^m(1 - 1/p)$. Moreover,

$$a_2(p^m) = \sum_{d_1 d_2 = p^m} d_2 = \sum_{i+j=m} p^i = \sum_{i=0}^{m} p^i = \frac{p^{m+1} - 1}{p - 1} = \frac{1 - 1/p^{m+1}}{1 - 1/p},$$

so $D_2(p^m) = (1 - 1/p)^2/(1 - 1/p^{m+1})$. Therefore

$$\left(1 - \frac{1}{p}\right)^2 \leq D_2(p^m) \leq 1 - \frac{1}{p}.$$

Since D_2 is multiplicative, we get

$$\left[\prod_{p|k} \left(1 - \frac{1}{p}\right)\right]^2 \leq D_2(k) \leq \prod_{p|k} \left(1 - \frac{1}{p}\right).$$

The left and right sides both tend to 0 if and only if $\lim_{i\to\infty} \sum_{p|k_i} 1/p \to \infty$, and they both converge to 1 if and only if $\lim_{i\to\infty} \sum_{p|k_i} 1/p \to 0$. $\square$

Appendix A. Calculation of a measure

In [Kat93] the asymptotics

$$N_{n,0}(T) = \frac{n-1}{\zeta(n)} w(B) T^{n(n-1)} \log T + O(T^{n(n-1)})$$

are given, where B is the unit ball in $M_n(\mathbb{R})$. The measure w on $M_n(\mathbb{R})$ is defined in [Kat93] as follows. Let $A_u := \{A \in M_n(\mathbb{R}) : Au = 0\}$ be the space of matrices annihilating the nonzero vector $u \in \mathbb{R}^n \setminus \{0\}$. We define for (Lebesgue measurable) subsets $E \subseteq M_n(\mathbb{R})$ the measure $w_u(E) := \mathrm{vol}(E \cap A_u)$ where vol is the standard $n(n-1)$-dimensional volume on A_u, and define the measure $w(E) := (1/2) \int_{\mathrm{S}^{n-1}} w_u(E)\, d\nu(u)$, where ν is the standard Euclidean surface measure on the $(n-1)$-dimensional sphere S^{n-1}.

We shall now calculate $w(B)$. The set $B \cap A_u$ is the unit ball in the $n(n-1)$-dimensional vector space A_u. Its volume does not depend on $u \neq 0$, and if $u = (0, \ldots, 0, 1)$, then $B \cap A_u$ is the unit ball in $\mathbb{R}^{n(n-1)}$, when identifying $M_n(\mathbb{R})$ with $\mathbb{R}^{n^2}$. Denote by $V_{n(n-1)}$ the volume of the unit ball in $\mathbb{R}^{n(n-1)}$. Thus $w_u(B) = V_{n(n-1)}$, independently of $u \neq 0$, and

$$w(B) = V_{n(n-1)} \frac{1}{2} \int_{\mathrm{S}^{n-1}} d\nu(u) = \frac{V_{n(n-1)} S_{n-1}}{2},$$

where S_{n-1} is the surface area of the sphere S^{n-1}. The volume and surface area of the unit ball is well known, and we may explicitly calculate

$$C_0 := w(B) = \frac{\pi^{n^2/2}}{\Gamma\left(\frac{n}{2}\right) \Gamma\left(\frac{n(n-1)}{2} + 1\right)}.$$

Recalling from Theorem 4 the expression for C_1, we get the following relation.

$$C_1 = \frac{1}{\zeta(2)\cdots\zeta(n)} \frac{\pi^{n^2/2}}{\Gamma\left(\frac{n}{2}\right)\Gamma\left(\frac{n(n-1)}{2}+1\right)} = \frac{1}{\zeta(2)\cdots\zeta(n)} C_0.$$

References

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[DRS93] W. Duke, Z. Rudnick, and P. Sarnak. Density of integer points on affine homogeneous varieties. *Duke Math. J.*, 71(1):143–179, 1993.

[GN10] Alexander Gorodnik and Amos Nevo. *The ergodic theory of lattice subgroups*, volume 172 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2010.

[Kat93] Y. R. Katznelson. Singular matrices and a uniform bound for congruence groups of $\mathrm{SL}_n(\mathbb{Z})$. *Duke Math. J.*, 69(1):121–136, 1993.

[Sie45] Carl Ludwig Siegel. A mean value theorem in geometry of numbers. *Ann. of Math. (2)*, 46:340–347, 1945.

[Sta97] Richard P. Stanley. *Enumerative combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[Wig05] Igor Wigman. Counting singular matrices with primitive row vectors. *Monatsh. Math.*, 144(1):71–84, 2005.